ソフトウェアのインストールを必要としないNIC型セキュリティ機構

Bubo：マルウェアの先を行く動的解析フレームワーク

上田 侑真（慶應義塾大学）

Buboとは？

監視対象に一切のソフトウェア的変更を要求しないハードウェアベースの動的解析フレームワーク

なぜBuboなのか？

マルウェアに対策されないセキュリティ機構の要件

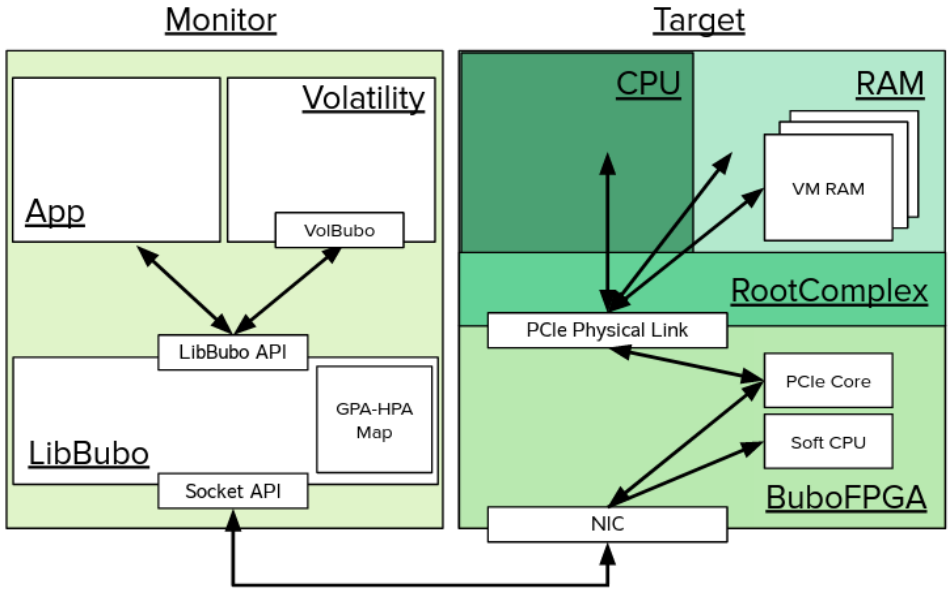
- 自信の存在を検知されないこと
- 情報を取得する際の高い完全性

Bubo

- 一切ソフトウェア的変更を加えない
- ハードウェアの持つ特権的な視点

結果、Buboは非常に対策されにくい。

また、Buboは現状、物理マシン、
仮想マシンのメモリ空間、I/Oを一切の
ソフトウェア的変更なしに監視できる
唯一のフレームワークである。



Buboで何が出来るのか？

- 遠隔の物理マシン、仮想マシンのメモリ空間をハードウェアによって取得できる
- 遠隔の物理マシン、仮想マシンのメモリ空間に直接Volatilityプラグインを実行できる
- PCI Expressデバイスのエミュレーションによる I/Oの監視ができる
- これまでにないマルウェアに対策されにくいセキュリティ機構を容易に実装できる

```
cyan@corep3 ~/m/volatility> ./vol.py -l bubo://bubofpga/0 imageinfo | head
Volatility Foundation Volatility Framework 2.6.1
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x86_23418, Win7SP0x86, Win7SP1x86_2
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : BuboFpgaAddressSpace (Unnamed AS)
                      PAE type : PAE
                           DTB : 0x185080L
                          KDBG : 0x82929be8L
          Number of Processors : 2
     Image Type (Service Pack) : 0
cyan@corep3 ~/m/volatility>
```

監視対象のホスト中の仮想マシンのメモリ空間に、Bubo経由で直接Volatilityプラグインを実行